Groups Geom. Dyn. 5 (2011), 509–527
DOI 10.4171/GGD/137

Groups, Geometry, and Dynamics

Words and mixing times in finite simple groups

Gili Schul and Aner Shalev

To Fritz, with fond memory

Abstract. Let $w \neq 1$ be a non-trivial group word, let G be a finite simple group, and let $w(G)$ be the set of values of w in G. We show that if G is large, then the random walk on G with respect to $w(G)$ as a generating set has mixing time 2.

This strengthens various known results, for example the fact that $w(G)^2$ covers almost all of G.

Mathematics Subject Classification (2010). 20D06, 20P99.

Keywords. Words, random walks, finite simple groups, mixing time.

1. Introduction

Let $w = w(x_1, \dots, x_d)$ be a non-trivial group word, namely a non-identity element of the free group F_d on $x_1, \dots, x_d$. Then we may write $w = x_{i_1}^{n_1} x_{i_2}^{n_2} \dots x_{i_k}^{n_k}$ where $i_j \in \{1, \dots, d\}$ and n_j are integers. Let G be a group. For $g_1, \dots, g_d \in G$ we write $w(g_1, \dots, g_d) = g_{i_1}^{n_1} g_{i_2}^{n_2} \dots g_{i_k}^{n_k} \in G$. Denote $w(G) = \{w(g_1, \dots, g_d) \mid g_1, \dots, g_d \in G\}$, the set of values of w in G. Also, for every subset $A \subseteq G$ we write $A^k = \{a_1 \dots a_k \mid a_i \in G\}$.

An interesting much studied question is how large $w(G)$ is for G a (nonabelian) finite simple group. In [La] it is shown that if $G_1, G_2, \dots$ is an infinite sequence of finite simple groups, no two of which are isomorphic, then

$$\lim_{i \to \infty} \frac{\log |w(G_i)|}{\log |G_i|} = 1.$$

Stronger results were subsequently obtained in [LaSh1] and in [NiPy].

Related Waring type problems were also widely studied, where the goal is to express each group element as a short product of values of w; see [LiSh1], [Sh], [Sh1], [LaSh1], [LaSh2], [NiPy]. In [Sh] it is shown that for every group word $w \neq 1$, there exists a positive integer $N = N(w)$ such that for every finite simple group G with $|G| \geq N(w)$ we have $w(G)^3 = G$.

In [LaSh1] and [LaSh2] a better result for alternating groups is proved. It is shown that if w_1, w_2 are non-trivial group words, then there exists $N = N(w_1, w_2)$ such that for all integers $n \geq N$ we have $w_1(A_n)w_2(A_n) = A_n$.

In this paper we focus on random walks on finite simple groups G with respect to $w(G)$ as a generating set. Our goal is to determine the mixing time of the random walk, namely the time required until we reach an almost uniform distribution on G. Our main theorem states that (when $|G|$ is large) this mixing time is the smallest possible, namely 2.

To make this precise, denote by U_G the uniform distribution on G, i.e., $U_G(g) = \frac{1}{|G|}$ for all $g \in G$. For $W \subseteq G$, denote by P_W the uniform distribution on W, i.e., $P_W(g) = \frac{1}{|W|}$ if $g \in W$ and 0 otherwise.

Denote by $P_W * P_W$ the convolution of the probability P_W with itself. Then $(P_W * P_W)(g)$ is the probability that $xy = g$ where $x, y \in W$ are chosen randomly, uniformly and independently.

For two distributions P, Q on G we let

$$\|P - Q\|_1 = \sum_{g \in G} |P(g) - Q(g)|$$

denote the L_1-distance between P and Q.

Theorem 1.1. *Fix a word $w \neq 1$, and let G be a finite simple group. Then $\|P_{w(G)} * P_{w(G)} - U_G\|_1 \to 0$ as $|G| \to \infty$.*

In fact the same method establishes a similar result for

$$\|P_{w_1(G)} * P_{w_2(G)} - U_G\|_1,$$

where w_1, w_2 are two non-trivial group words.

This result for alternating groups has recently been obtained in [LaSh2]. It remains to prove it for groups of Lie type, which is what we do here.

From Theorem 1.1 one can deduce that $w(G)^2$ covers almost all of G for G a finite simple group and w a non-trivial group word. This has already been proved in Corollary 1.4 of [Sh1].

In fact we prove a more general result of independent interest. Recall that a normal subset of a group G is a subset closed under conjugation (namely a union of conjugacy classes).

If G is a simple group of Lie type then the rank r of G is defined to be the rank of the ambient simple algebraic group, unless we deal with Lie types ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$, in which case $r = 1, 1, 2$, respectively.

Theorem 1.2. *Let G be a finite simple group of Lie type of rank r over a field with q elements. Let $W \subseteq G$ be a normal subset. Then for any $\varepsilon > 0$ there exists a* *number* $R(\varepsilon)$ *depending only on* ε *such that if* $r > R(\varepsilon)$ *and* $|W|/|G| \geq q^{-r(1-\varepsilon)}$, *or if* $r \leq R(\varepsilon)$ *and* $|W|/|G| \geq q^{-(1-\varepsilon)}$, *then*

$$\|P_W * P_W - U_G\|_1 \to 0 \quad \text{as } |G| \to \infty.$$

Combining this result with known estimates on the size of $w(G)$ we then deduce Theorem 1.1.

In fact we prove a more general result on k normal subsets $W_1, \dots, W_k$ and give sufficient conditions for

$$\|P_{W_1} * \cdots * P_{W_k} - U_G\|_1 \to 0.$$

See Theorems 3.3 and 3.5 bellow.

In our proofs we use character theory. To understand the relevance, let G be a finite group, $g \in G$, and let $C_i = x_i^G$ $(i = 1, \dots, k)$ be conjugacy classes. Let $P_{C_1,\dots,C_k}(g)$ denote the probability that $y_1 \dots y_k = g$ where $y_i \in C_i$ are chosen randomly and uniformly. Notice that $P_{C_1,\dots,C_k} = P_{C_1} * \cdots * P_{C_k}$. Let Irr G denote the set of complex irreducible characters of G. It follows from a classical result that

$$P_{C_1,\dots,C_k}(g) = |G|^{-1} \sum_{\chi \in \operatorname{Irr} G} \frac{\chi(x_1) \dots \chi(x_k) \chi(g^{-1})}{\chi(1)^{k-1}}.$$

For a proof of this result see for instance Theorem 30.4 of [JaLi].

We also use the Witten zeta function ζ_G encoding the character degrees of a finite group G. For a real number s define

$$\zeta_G(s) = \sum_{\chi \in \operatorname{Irr} G} \chi(1)^{-s}.$$

We use the fact established in [LiSh2] that for a finite simple group G, $\zeta_G(2) \to 1$ as $|G| \to \infty$.

Throughout, c_i denote suitable positive absolute constants.

Acknowledgement. We would like to thank the Israel Science Foundation for supporting this research via Grant 754/08.

2. Preliminaries

In proving our results we use known estimates for the size of $w(G)$.

The first result in this direction is Proposition 7 of [La]:

Theorem 2.1. *For any non-trivial word* w *and any root system* Φ, *there exists a constant* $c = c(w, \Phi) > 0$ *such that*

$$|w(G)| > c|G|$$

for all simple groups G *of Lie type associated to the root system* Φ.

Theorem 1.11 of [LaSh1] states:

Theorem 2.2. *Let G be a finite simple group of Lie type and of rank r. Let $w \neq 1$ be a word. Then if G is not of type A_r or ${}^2A_r$, we have*

$$|w(G)| \geq cr^{-1}|G|$$

for some absolute constant $c > 0$, provided $|G| \geq N(w)$.

For groups of type A_r we use Proposition 1.7 of [NiPy]:

Theorem 2.3. *Given w there is a constant $c = c(w) > 0$, depending only in w, such that if $G = \mathrm{SL}(n,q)$ then*

$$|w(G)| > \frac{c|G|}{n^3 q^{24+n/4}}.$$

For groups of type ${}^2A_r$ we use Proposition 1.8 of [NiPy]:

Theorem 2.4. *Let $L = \mathrm{SU}(d,q)$. There is a constant $e > 0$ such that*

$$|w(L)| > \frac{e|L|}{d^3 q^{49+d/4}}.$$

Using these three results it is easy to deduce the following:

Theorem 2.5. *Let $G = G_r(q)$ be a finite simple group of Lie type of rank r over the field with q elements. Let w be a group word. There are integers $N = N(w)$ and $R = R(w)$ such that if $|G| \geq N$ and $r \geq R$, then $\frac{|w(G)|}{|G|} \geq q^{-\frac{r}{3}}$.*

All these theorems suggest that $w(G)$ is a large normal subset, and we would like to evaluate

$$\|P_W * \cdots * P_W - U_G\|_1^2,$$

for large normal subsets W. We can split W into conjugacy classes $C_i = x_i^G$. A classical result states

$$P_{C_1,\ldots,C_k}(g) = |G|^{-1} \sum_{\chi \in \mathrm{Irr}\, G} \frac{\chi(x_1)\ldots\chi(x_k)\chi(g^{-1})}{\chi(1)^{k-1}}.$$

From this we deduce the following lemma, which is probably well known. For completeness we insert a proof.

Lemma 2.6. *Let G be a finite group, and let $C_i = x_i^G$ be conjugacy classes. Then*

$$\|P_{C_1} * \cdots * P_{C_k} - U_G\|_1^2 \leq \sum_{\substack{\chi \in \mathrm{Irr}\, G \\ \chi \neq 1}} \frac{|\chi(x_1)|^2 \ldots |\chi(x_k)|^2}{\chi(1)^{2k-2}}.$$

Proof.

$$\|P_{C_1} * \cdots * P_{C_k} - U_G\|_1^2 = \Big(\sum_{g\in G} |P_{C_1} * \cdots * P_{C_k}(g) - |G|^{-1}|\Big)^2$$
$$= \Big(\sum_{g\in G} \Big||G|^{-1} \sum_{\chi\in \mathrm{Irr}\, G} \frac{\chi(x_1)\ldots\chi(x_k)\chi(g^{-1})}{\chi(1)^{k-1}} - |G|^{-1}\Big|\Big)^2$$
$$= |G|^{-2}\Big(\sum_{g\in G}\Big|\sum_{1\neq\chi\in \mathrm{Irr}\, G} \frac{\chi(x_1)\ldots\chi(x_k)\chi(g^{-1})}{\chi(1)^{k-1}}\Big|\Big)^2.$$

By the Cauchy–Schwarz inequality we have,

$$|G|^{-2}\Big(\sum_{g\in G}\Big|\sum_{1\neq\chi\in \mathrm{Irr}\, G} \frac{\chi(x_1)\ldots\chi(x_k)\chi(g^{-1})}{\chi(1)^{k-1}}\Big|\Big)^2$$
$$\leq |G|^{-1}\sum_{g\in G}\Big|\sum_{1\neq\chi\in \mathrm{Irr}\, G} \frac{\chi(x_1)\ldots\chi(x_k)\chi(g^{-1})}{\chi(1)^{k-1}}\Big|^2$$
$$= |G|^{-1}\sum_{g\in G}\Big(\sum_{1\neq\chi\in \mathrm{Irr}\, G} \frac{\chi(x_1)\ldots\chi(x_k)\chi(g^{-1})}{\chi(1)^{k-1}}\Big)\overline{\Big(\sum_{1\neq\rho\in \mathrm{Irr}\, G} \frac{\rho(x_1)\ldots\rho(x_k)\rho(g^{-1})}{\rho(1)^{k-1}}\Big)}$$
$$= |G|^{-1}\sum_{g\in G}\sum_{\chi\neq 1}\sum_{\rho\neq 1} \frac{\chi(x_1)\overline{\rho(x_1)}\ldots\chi(x_k)\overline{\rho(x_k)}\chi(g^{-1})\overline{\rho(g^{-1})}}{\chi(1)^{k-1}\overline{\rho(1)^{k-1}}}$$
$$= |G|^{-1}\sum_{\chi\neq 1}\sum_{\rho\neq 1} \frac{\chi(x_1)\overline{\rho(x_1)}\ldots\chi(x_k)\overline{\rho(x_k)}}{\chi(1)^{k-1}\overline{\rho(1)^{k-1}}}\Big(\sum_{g\in G}\chi(g^{-1})\overline{\rho(g^{-1})}\Big)$$
$$= \sum_{1\neq\chi\in \mathrm{Irr}\, G} \frac{|\chi(x_1)|^2\ldots|\chi(x_k)|^2}{\chi(1)^{2k-2}}.$$

The last equality is by the orthogonality relations (see e.g. [Ser]). □

Now we use known results on the irreducible representations of finite simple groups of Lie type. By [LiSh3] Section 6 (see also Lemma 4.6 of [Sh]) we have:

Lemma 2.7. *Let $G = G_r(q)$ be a finite simple classical group. Then* $\mathrm{Irr}\, G$ *has a subset $\mathcal{W}$ of so called Weil characters with the following properties:*

(i) $|\mathcal{W}| \leq q + 1$.

(ii) *Let $\chi \in \mathcal{W}$ and $x \in G$. If $|C_G(x)| \leq q^m$ for some integer m, then $|\chi(x)| \leq q^{\sqrt{m+b}}$ where b is some absolute constant.*

(iii) *If $1 \neq \chi \in \mathrm{Irr}\, G \setminus \mathcal{W}$ and $r > 5$ then $\chi(1) \geq cq^{2r-3}$ where $c > 0$ is some absolute constant.*

We also use the following:

Lemma 2.8. *Let $G = G_r(q)$ be a finite simple group of Lie type of rank r over the field with q elements, and let $k(G)$ denote the number of conjugacy classes of G.*

(i) *There is a positive constant c_1 such that $\chi(1) \geq c_1 q^r$ for all $1 \neq \chi \in \mathrm{Irr}\, G$.*

(ii) *There is a positive constant c_2 such that $k(G) \leq c_2 q^r$.*

Proof. Part (i) follows from [LanSe] and (ii) from [FuGu]. □

Theorem 1.1 of [LiSh2] states:

Theorem 2.9. *Let G be a finite simple group, and for a real number s let*

$$\zeta_G(s) = \sum_{\chi \in \mathrm{Irr}\, G} \chi(1)^{-s}.$$

If $s > 1$ then $\zeta_G(s) \to 1$ as $|G| \to \infty$.

We also use known estimates for the number of regular semisimple elements. Recall that an element x of a finite group G of Lie type is called regular if its centralizer in the corresponding algebraic group $\overline{G}$ has minimal dimension, namely $\mathrm{rank}(\overline{G})$.

We say that x is semisimple if its order is not divisible by p, where p is the defining characteristic of G. The next result is of Guralnick and Lübeck in [GuLu]:

Theorem 2.10. *Let G be a finite simple group of Lie type over the field with q elements. Denote by $r(G)$ the proportion of regular semisimple elements in G. Then*

$$1 - r(G) < \frac{3}{q-1} + \frac{2}{(q-1)^2}.$$

From this theorem, using elementary computations, we easily obtain:

Corollary 2.11. *Let G be a finite simple group of Lie type over the field with q elements. Denote by $r(G)$ the proportion of regular semisimple elements in G. Then*

$$1 - r(G) < \frac{5}{q}.$$

So we can see that there are many regular semisimple elements, and we use the next lemma when dealing with these elements in groups of bounded rank:

Lemma 2.12. *Let $G = G_r(q)$ be a finite simple group of Lie type of rank r over the field with q elements, and let $x \in G$ be a regular semisimple element. Then there is a number $c = c(r)$, depending on r but not on q, such that $|\chi(x)| \leq c$ for all $\chi \in \mathrm{Irr}\, G$.*

Proof. This follows from the Deligne–Lusztig theory; see [Lus], and formula 4.26.1 in particular. □

3. Proofs

Lemma 3.1. *Let G be a finite group, $k \geq 2$ an integer, and let $x_1, x_2, \ldots, x_k \in G$ be elements of G. Then*

$$\sum_{\chi \in \operatorname{Irr} G} |\chi(x_1)\chi(x_2)\ldots\chi(x_k)| \leq |C_G(x_1)|^{\frac{1}{2}} |C_G(x_2)|^{\frac{1}{2}} \ldots |C_G(x_k)|^{\frac{1}{2}}.$$

Proof. By the orthogonality relations (see e.g. [Ser]) we have

$$\sum_{\chi \in \operatorname{Irr} G} |\chi(x_i)|^2 = |C_G(x_i)|.$$

In particular $|\chi(x_i)| \leq |C_G(x_i)|^{\frac{1}{2}}$ for all $1 \leq i \leq k$ and all $\chi \in \operatorname{Irr} G$. Clearly

$$\sum_{\chi \in \operatorname{Irr} G} |\chi(x_1)\chi(x_2)\ldots\chi(x_k)| \leq |C_G(x_3)|^{\frac{1}{2}} \ldots |C_G(x_k)|^{\frac{1}{2}} \sum_{\chi \in \operatorname{Irr} G} |\chi(x_1)\chi(x_2)|.$$

By the Cauchy–Schwarz inequality we have

$$\begin{aligned}\sum_{\chi \in \operatorname{Irr} G} |\chi(x_1)\chi(x_2)| &\leq \Big(\sum_{\chi \in \operatorname{Irr} G} |\chi(x_1)|^2\Big)^{\frac{1}{2}} \Big(\sum_{\chi \in \operatorname{Irr} G} |\chi(x_2)|^2\Big)^{\frac{1}{2}} \\ &= |C_G(x_1)|^{\frac{1}{2}} |C_G(x_2)|^{\frac{1}{2}}.\end{aligned}$$

The result now follows from the two inequalities above. □

Theorem 3.2. *Let $G = G_r(q)$ be a finite simple group of Lie type of rank r over the field with q elements. Let $k \geq 2$ be an integer. Let $\varepsilon > 0$ and let $x_1, x_2, \ldots, x_k \in G$ such that*

$$\prod_{i=1}^{k} |C_G(x_i)| \leq q^{(4k-4-(3-\frac{4}{k})\varepsilon)r}.$$

(i) *If $r > 5$ and G is a classical group, then*

$$\sum_{\substack{\chi \in \operatorname{Irr} G \\ \chi \neq 1}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} \leq 2c_1^{1-k} q^{k\sqrt{(4k-4)r+b} - r(k-1)+1} + c_2^{1-k} q^{3k-3-(1.5-\frac{2}{k})r\varepsilon},$$

where c_1, c_2 and b are absolute constants.

(ii) *There exists a real number $r_1 = r_1(k, \varepsilon)$ such that if $r \geq r_1$ then*

$$\sum_{\substack{\chi \in \operatorname{Irr} G \\ \chi \neq 1}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} \to 0 \quad \textit{as } |G| \to \infty.$$

Proof. We first prove (i).

Let $\mathcal{W}$ be the set of Weil characters of G (see 2.7). Set

$$\sum_{\substack{\chi\in \mathrm{Irr}\, G\\ \chi\neq 1}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} = \sum_{\chi\in\mathcal{W}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} + \sum_{\substack{\chi\notin\mathcal{W}\\ \chi\neq 1}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}}.$$

We will handle each summand separately.

The first summand:

From our assumptions $|C_G(x_i)| \leq q^{(4k-4)r}$ and so (ii) of Lemma 2.7 yields $|\chi(x_i)| \leq q^{\sqrt{(4k-4)r+b}}$ for $i = 1,\ldots,k$ and $\chi\in\mathcal{W}$. We also have $\chi(1)\geq c_1 q^r$ for all non-trivial $\chi\in \mathrm{Irr}\, G$ (i) of Lemma 2.8. Therefore

$$\sum_{\chi\in\mathcal{W}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} \leq \sum_{\chi\in\mathcal{W}} \frac{q^{k\sqrt{(4k-4)r+b}}}{\chi(1)^{k-1}} \leq \frac{|\mathcal{W}|q^{k\sqrt{(4k-4)r+b}}}{c_1^{k-1}q^{(k-1)r}}.$$

From (i) of Lemma 2.7 we have $|\mathcal{W}|\leq q+1$ and so

$$\begin{aligned}\sum_{\chi\in\mathcal{W}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} &\leq \frac{(q+1)q^{k\sqrt{(4k-4)r+b}}}{c_1^{k-1}q^{(k-1)r}}\\ &\leq \frac{2q\cdot q^{k\sqrt{(4k-4)r+b}}}{c_1^{k-1}q^{(k-1)r}}\\ &= 2c_1^{1-k}q^{k\sqrt{(4k-4)r+b}-(k-1)r+1}.\end{aligned}$$

The second summand:

If $1\neq\chi\notin\mathcal{W}$ and $r>5$, (iii) of Lemma 2.7 yields $\chi(1)\geq c_2q^{2r-3}$. Hence

$$\begin{aligned}\sum_{\substack{\chi\notin\mathcal{W}\\ \chi\neq 1}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} &\leq c_2^{1-k}q^{(1-k)(2r-3)}\sum_{\substack{\chi\notin\mathcal{W}\\ \chi\neq 1}} |\chi(x_1)\ldots\chi(x_k)|\\ &\leq c_2^{1-k}q^{(1-k)(2r-3)}\sum_{\chi\in \mathrm{Irr}\, G} |\chi(x_1)\ldots\chi(x_k)|.\end{aligned}$$

Using Lemma 3.1 we obtain

$$\sum_{\substack{\chi\notin\mathcal{W}\\ \chi\neq 1}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} \leq c_2^{1-k}q^{(1-k)(2r-3)}|C_G(x_1)|^{\frac{1}{2}}\ldots|C_G(x_k)|^{\frac{1}{2}}.$$

Using our assumption on $|C_G(x_1)|\ldots|C_G(x_k)|$ we obtain

$$\begin{aligned}\sum_{\substack{\chi\notin\mathcal{W}\\ \chi\neq 1}} \frac{|\chi(x_1)\ldots\chi(x_k)|}{\chi(1)^{k-1}} &\leq c_2^{1-k}q^{(1-k)(2r-3)}q^{(2k-2-(1.5-\frac{2}{k})\varepsilon)r}\\ &= c_2^{1-k}q^{3k-3-(1.5-\frac{2}{k})r\varepsilon}.\end{aligned}$$

The sum:

We conclude that for $r > 5$ and for G a classical group,

$$\sum_{\substack{\chi \in \operatorname{Irr} G \\ \chi \neq 1}} \frac{|\chi(x_1)\dots\chi(x_k)|}{\chi(1)^{k-1}} \leq 2c_1^{1-k} q^{k\sqrt{(4k-4)r+b}-(k-1)r+1} + c_2^{1-k} q^{3k-3-(1.5-\frac{2}{k})r\varepsilon},$$

proving (i).

Since the simple groups of Lie type which are not classical are of rank at most 8, we can use (i) by assuming also $r > 8$.

Hence, if $r > 8$ and also large enough so that

$$k\sqrt{(4k-4)r+b} - (k-1)r + 1 < 0$$

and

$$3k - 3 - (1.5 - \tfrac{2}{k})r\varepsilon < 0,$$

then

$$\sum_{\substack{\chi \in \operatorname{Irr} G \\ \chi \neq 1}} \frac{|\chi(x_1)\dots\chi(x_k)|}{\chi(1)^{k-1}} \to 0 \quad \text{as } |G| \to \infty,$$

proving (ii). □

Theorem 3.3. *Let G be a finite simple group of Lie type of rank r over the field with q elements. Let $k \geq 2$ be an integer. Let $0 < \varepsilon$. Let $W_1, \dots, W_k$ be normal subsets such that*

$$\frac{|W_i|}{|G|} \geq q^{-(3-\frac{4}{k})r(1-\varepsilon)}.$$

Then there exists a real number $r_1 = r_1(k, \varepsilon)$ such that the following holds.

(i) *If $r \geq r_1$ and $|G| \geq N = N(k, \varepsilon)$, where N is an integer that depends only on k and ε, then*

$$\begin{aligned}\|P_{W_1} * \dots * P_{W_k} - U_G\|_1 &\\ \leq \sqrt{2c_1^{1-k} q^{k\sqrt{(4k-4)r+b}-r(k-1)+1} + c_2^{1-k} q^{3k-3-(1.5-\frac{2}{k})r\varepsilon}} &\\ + (2^k - 1)2c_3 q^{-(3-\frac{4}{k})\frac{k-1}{k}\varepsilon r}, &\end{aligned}$$

where c_1, c_2, c_3, b are absolute constants.

(ii) *If $r \geq r_1$ then $\left\| P_{W_1} * \dots * P_{W_k} - U_G \right\|_1 \to 0$ as $|G| \to \infty$.*

Proof. Partition W_i into two subsets $W_{i,1}$ and $W_{i,2}$ as follows:

$$W_{i,1} = \left\{x \in W_i : |C_G(x)| \leq q^{(4-\frac{4}{k}-\frac{(3k-4)\varepsilon}{k^2})r}\right\}$$

$$W_{i,2} = \left\{x \in W_i : |C_G(x)| > q^{(4-\frac{4}{k}-\frac{(3k-4)\varepsilon}{k^2})r}\right\}.$$

Then $W_{i,1}$ and $W_{i,2}$ are normal subsets, and

$$W_i = W_{i,1} \cup W_{i,2}, \quad W_{i,1} \cap W_{i,2} = \phi.$$

Hence,

$$P_{W_i} = \frac{|W_{i,1}|}{|W_i|} P_{W_{i,1}} + \frac{|W_{i,2}|}{|W_i|} P_{W_{i,2}}.$$

It follows that

$$\begin{aligned} P_{W_1} * \cdots * P_{W_k} \\ &= \left(\frac{|W_{1,1}|}{|W_1|} P_{W_{1,1}} + \frac{|W_{1,2}|}{|W_1|} P_{W_{1,2}} \right) * \cdots * \left(\frac{|W_{k,1}|}{|W_k|} P_{W_{k,1}} + \frac{|W_{k,2}|}{|W_k|} P_{W_{k,2}} \right) \\ &= \sum_{(j_1,\ldots,j_k)\in\{1,2\}^k} \left(\frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \right) P_{W_{1,j_1}} * \cdots * P_{W_{k,j_k}}. \end{aligned}$$

Since

$$U_G = \sum_{(j_1,\ldots,j_k)\in\{1,2\}^k} \left(\frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \right) U_G,$$

we have

$$\begin{aligned} \| P_{W_1} * \cdots * P_{W_k} - U_G \|_1 \\ &\leq \sum_{(j_1,\ldots,j_k)\in\{1,2\}^k} \frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \| P_{W_{1,j_1}} * \cdots * P_{W_{k,j_k}} - U_G \|_1. \end{aligned} \tag{1}$$

We will handle the first summand

$$\frac{|W_{1,1}|}{|W_1|} \cdots \frac{|W_{k,1}|}{|W_k|} \| P_{W_{1,1}} * \cdots * P_{W_{k,1}} - U_G \|_1$$

differently from the other $2^k - 1$ summands.

The first summand:

$$\frac{|W_{1,1}|}{|W_1|} \cdots \frac{|W_{k,1}|}{|W_k|} \| P_{W_{1,1}} * \cdots * P_{W_{k,1}} - U_G \|_1 \leq \| P_{W_{1,1}} * \cdots * P_{W_{k,1}} - U_G \|_1.$$

$W_{i,1}$ is a normal subset, and hence is a union of conjugacy classes. Denote the conjugacy classes of $W_{i,1}$ by $C_{i,1}, \ldots C_{i,m_i}$. So $W_{i,1} = \bigcup_{j=1}^{m_i} C_{i,j}$.

Hence,

$$\begin{aligned} P_{W_{1,1}} * \cdots * P_{W_{k,1}} &= \left(\sum_{j_1=1}^{m_1} \frac{|C_{1,j_1}|}{|W_{1,1}|} P_{C_{1,j_1}} \right) * \cdots * \left(\sum_{j_k=1}^{m_k} \frac{|C_{k,j_k}|}{|W_{k,1}|} P_{C_{k,j_k}} \right) \\ &= \sum_{\substack{1 \leq j_1 \leq m_1 \\ \cdots \\ 1 \leq j_k \leq m_k}} \frac{|C_{1,j_1}| \ldots |C_{k,j_k}|}{|W_{1,1}| \ldots |W_{k,1}|} P_{C_{1,j_1}} * \cdots * P_{C_{k,j_k}}. \end{aligned}$$

Therefore,

$$\|P_{W_{1,1}}*\cdots*P_{W_{k,1}}-U_G\|_1 \le \sum_{\substack{1\le j_1\le m_1\\ \cdots\\ 1\le j_k\le m_k}} \frac{|C_{1,j_1}|\ldots|C_{k,j_k}|}{|W_{1,1}|\ldots|W_{k,1}|}\|P_{C_{1,j_1}}*\cdots*P_{C_{k,j_k}}-U_G\|_1.$$

According to Lemma 2.6,

$$\|P_{C_{1,j_1}}*\cdots*P_{C_{k,j_k}}-U_G\|_1^2 \le \sum_{\substack{\chi\in\mathrm{Irr}\,G\\ \chi\ne 1}} \frac{|\chi(x_{1,j_1})|^2\ldots|\chi(x_{k,j_k})|^2}{\chi(1)^{2k-2}},$$

where $C_{i,j_i}=x_{i,j_i}^G$.

Any $x_{1,j_1},\ldots,x_{k,j_k}$ satisfy

$$|C_G(x_{1,j_1})|\ldots|C_G(x_{k,j_k})| \le \left(q^{(4-\frac{4}{k}-\frac{(3k-4)\varepsilon}{k^2})r}\right)^k = q^{(4k-4-(3-\frac{4}{k})\varepsilon)r}.$$

Hence, according to Theorem 3.2, if $r\ge r_1$ then

$$\sum_{\substack{\chi\in\mathrm{Irr}\,G\\ \chi\ne 1}} \frac{|\chi(x_{1,j_1})|\ldots|\chi(x_{k,j_k})|}{\chi(1)^{k-1}} \to 0$$

as $|G|\to\infty$.

In particular there exists $N=N(k,\varepsilon)$ such that if $|G|\ge N$ then for any $\chi\ne 1$ we have

$$\frac{|\chi(x_{1,j_1})|\ldots|\chi(x_{k,j_k})|}{\chi(1)^{k-1}} \le 1.$$

Hence, if $r\ge r_1$ and $|G|\ge N$ then,

$$\begin{aligned}\sum_{\substack{\chi\in\mathrm{Irr}\,G\\ \chi\ne 1}} \frac{|\chi(x_{1,j_1})|^2\ldots|\chi(x_{k,j_k})|^2}{\chi(1)^{2k-2}} &\le \sum_{\substack{\chi\in\mathrm{Irr}\,G\\ \chi\ne 1}} \frac{|\chi(x_{1,j_1})|\ldots|\chi(x_{k,j_k})|}{\chi(1)^{k-1}}\\ &\le 2c_1^{1-k}q^{k\sqrt{(4k-4)r+b}-r(k-1)+1}\\ &\quad + c_2^{1-k}q^{3k-3-(1.5-\frac{2}{k})r\varepsilon}.\end{aligned}$$

The last inequality is from Theorem 3.2.

Therefore,

$$\begin{aligned}&\|P_{C_{1,j_1}}*\cdots*P_{C_{k,j_k}}-U_G\|_1\\ &\quad\le \sqrt{\sum_{\substack{\chi\in\mathrm{Irr}\,G\\ \chi\ne 1}} \frac{|\chi(x_{1,j_1})|^2\ldots|\chi(x_{k,j_k})|^2}{\chi(1)^{2k-2}}}\\ &\quad\le \sqrt{2c_1^{1-k}q^{k\sqrt{(4k-4)r+b}-r(k-1)+1}+c_2^{1-k}q^{3k-3-(1.5-\frac{2}{k})r\varepsilon}}.\end{aligned}$$

Hence, when $r \geq r_1$ and $|G| \geq N$ then

$$\begin{aligned}
&\| P_{W_{1,1}} * \cdots * P_{W_{k,1}} - U_G \|_1 \\
&\quad \leq \sum_{\substack{1 \leq j_1 \leq m_1 \\ \cdots \\ 1 \leq j_k \leq m_k}} \frac{|C_{1,j_1}| \ldots |C_{k,j_k}|}{|W_{1,1}| \ldots |W_{k,1}|} \| P_{C_{1,j_1}} * \cdots * P_{C_{k,j_k}} - U_G \|_1 \\
&\quad \leq \sqrt{2c_1^{1-k} q^{k\sqrt{(4k-4)r+b} - r(k-1)+1} + c_2^{1-k} q^{3k-3-(1.5-\frac{2}{k})r\varepsilon}}.
\end{aligned}$$

The other $2^k - 1$ *summands:*
Each summand is of the form

$$\frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \| P_{W_{1,j_1}} * \cdots * P_{W_{k,j_k}} - U_G \|_1,$$

where $j_1, \ldots, j_k \in \{1, 2\}$ and at least one of $j_1, \ldots, j_k$ equals 2.
Since $\| P - Q \|_1 \leq 2$ for distributions P and Q, we have

$$\frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \| P_{W_{1,j_1}} * \cdots * P_{W_{k,j_k}} - U_G \|_1 \leq 2 \frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|}.$$

Denote

$$S = \left\{ x \in G : |C_G(x)| \geq q^{(4 - \frac{4}{k} - \frac{(3k-4)\varepsilon}{k^2})r} \right\}.$$

Denote by $k(G)$ the number of conjugacy classes in G. Then S is a normal subset, which splits into at most $k(G)$ conjugacy classes, and each conjugacy class is of size at most

$$|G| q^{(-4 + \frac{4}{k} + \frac{(3k-4)\varepsilon}{k^2})r}.$$

Hence

$$|S| \leq k(G) |G| q^{(-4 + \frac{4}{k} + \frac{(3k-4)\varepsilon}{k^2})r}.$$

According to (ii) of Lemma 2.8:

$$k(G) \leq c_3 q^r$$

where c_3 is an absolute constant. So

$$|S| \leq c_3 |G| q^{(-3 + \frac{4}{k} + \frac{(3k-4)\varepsilon}{k^2})r} = c_3 |G| q^{-(3 - \frac{4}{k}) r (1 - \frac{\varepsilon}{k})}.$$

Since $W_{i,2} \subseteq S$ we obtain

$$\frac{|W_{i,2}|}{|G|} \leq c_3 q^{-(3 - \frac{4}{k}) r (1 - \frac{\varepsilon}{k})}$$

for $1 \leq i \leq k$.

We are assuming $\frac{|W_i|}{|G|} \geq q^{-(3-\frac{4}{k})r(1-\varepsilon)}$.
Hence

$$\frac{|W_{i,2}|}{|W_i|} = \frac{\frac{|W_{i,2}|}{|G|}}{\frac{|W_i|}{|G|}} \leq c_3 q^{-(3-\frac{4}{k})r(1-\frac{\varepsilon}{k})+(3-\frac{4}{k})r(1-\varepsilon)} = c_3 q^{-(3-\frac{4}{k})\frac{k-1}{k}\varepsilon r}.$$

Since at least one of $j_1, \ldots, j_k$ equals 2,

$$\frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \leq c_3 q^{-(3-\frac{4}{k})\frac{k-1}{k}\varepsilon r},$$

and so

$$\begin{aligned}\frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \|P_{W_{1,j_1}} * \cdots * P_{W_{k,j_k}} - U_G\|_1 &\leq 2\frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \\ &\leq 2c_3 q^{-(3-\frac{4}{k})\frac{k-1}{k}\varepsilon r}.\end{aligned}$$

The sum:
When $r \geq r_1$ and $|G| \geq N$ we obtain

$$\begin{aligned}&\|P_{W_1} * \cdots * P_{W_k} - U_G\|_1 \\ &\leq \sum_{(j_1,\ldots,j_k)\in\{1,2\}^k} \frac{|W_{1,j_1}|}{|W_1|} \cdots \frac{|W_{k,j_k}|}{|W_k|} \left\|P_{W_{1,j_1}} * \cdots * P_{W_{k,j_k}} - U_G\right\|_1 \\ &\leq \sqrt{2c_1^{1-k} q^{k\sqrt{(4k-4)r+b}-r(k-1)+1} + c_2^{1-k} q^{3k-3-(1.5-\frac{2}{k})r\varepsilon}} \\ &\quad + (2^k-1)2c_3 q^{-(3-\frac{4}{k})\frac{k-1}{k}\varepsilon r},\end{aligned}$$

proving (i). Part (ii) is an immediate consequence. □

We now draw conclusions for sets $w(G)$ of word values.

Theorem 3.4. *Let $w \neq 1$ be a non-trivial group word. Let $G = G_r(q)$ be a finite simple group of Lie type of rank r over the field with q elements. Then there is an integer $r_0(w)$, depending only on w, such that the following holds.*

(i) *If $r \geq r_0(w)$ and $|G| \geq N(w)$, where $N(w)$ depends only on w, then*

$$\|P_{w(G)} * P_{w(G)} - U_G\|_1 \leq \sqrt{2c_1^{-1} q^{2\sqrt{4r+b}-r+1} + c_2^{-1} q^{3-\frac{r}{3}}} + 6c_3 q^{-\frac{r}{3}},$$

where c_1, c_2, c_3, b are absolute constants.

(ii) *If $r \geq r_0(w)$ then $\|P_{w(G)} * P_{w(G)} - U_G\|_1 \to 0$ as $|G| \to \infty$.*

Proof. We will deal separately with the different types of groups G to show that for r large enough and $|G|$ large enough we have $\frac{|w(G)|}{|G|} \geq q^{-\frac{r}{3}}$.

G is not of type A_r or ${}^2A_r$:

According to Theorem 2.2, there is an absolute constant $c > 0$ and an integer $M(w)$, such that if $|G| \geq M(w)$ then

$$\frac{|w(G)|}{|G|} \geq c \cdot r^{-1}.$$

There exists an absolute constant r_2 (that depends only on the absolute constant c) such that for $r \geq r_2$, we have $c \cdot r^{-1} \geq 2^{-\frac{r}{3}}$. So for $r \geq r_2$ and $|G| \geq M(w)$ we have

$$\frac{|w(G)|}{|G|} \geq c \cdot r^{-1} \geq 2^{-\frac{r}{3}} \geq q^{-\frac{r}{3}}.$$

G is of type A_r:

According to Theorem 2.3, if $G = \mathrm{SL}(r+1, q)$, and given w, there is an integer $d(w) > 0$, depending only on w, such that

$$\frac{|w(G)|}{|G|} > \frac{d(w)}{(r+1)^3 q^{24+\frac{r+1}{4}}}.$$

For $G = \mathrm{PSL}(r+1, q)$ we also have this inequality, since for a subset $S \subseteq G$ we have

$$\frac{|\overline{S}|}{|\overline{G}|} = \frac{|\overline{S}|}{|G|/|N|} \geq \frac{|S|/|N|}{|G|/|N|} = \frac{|S|}{|G|},$$

where $N = Z(G)$, $\overline{G} = G/N$ and $\overline{S} = SN/N$.

So for r larger than a constant $r_3(w)$ that depends only on $d(w)$ (and therefore only on w) we have

$$\frac{|w(G)|}{|G|} > q^{-\frac{r}{3}}.$$

G is of type ${}^2A_r$:

In this case the argument is similar to the case of A_r using Theorem 2.4 in place of Theorem 2.3. Hence there is a constant $r_4(w)$ such that if $r \geq r_4(w)$ then $\frac{|w(G)|}{|G|} > q^{-\frac{r}{3}}$.

Conclusion:

If $G = G_r(q)$ is a finite simple group of Lie type, and w is a group word, there are integers $M(w)$ and $r_2, r_3(w), r_4(w)$ such that if $|G| \geq M(w)$ and $r \geq \max\{r_2, r_3(w), r_4(w)\}$, then $\frac{|w(G)|}{|G|} \geq q^{-\frac{r}{3}}$.

Now we can use Theorem 3.3 with $\varepsilon = \frac{2}{3}$ and $k = 2$ and obtain:

If $r \geq \max\{r_1(2, \frac{2}{3}), r_2, r_3(w), r_4(w)\}$ and $|G| \geq \max\{N(\frac{2}{3}), M(w)\}$ then,

$$\|P_{w(G)} * P_{w(G)} - U_G\|_1 \leq \sqrt{2c_1^{-1}q^{2\sqrt{4r+b}-r+1} + c_2^{-1}q^{3-\frac{r}{3}}} + 6c_3 q^{-\frac{r}{3}},$$

where c_1, c_2, c_3, b are absolute constants.

Part (ii) is an immediate consequence. □

Theorem 3.5. *Let G be a finite simple group of Lie type of rank r over the field with q elements. Let $0 < \varepsilon < 1$. Let W_1, W_2 be normal subsets such that*

$$\frac{|W_i|}{|G|} \geq q^{-(1-\varepsilon)} \quad \textit{for } i = 1, 2.$$

Then:

(i) $\|P_{W_1} * P_{W_2} - U_G\|_1 \leq \sqrt{d(r) \cdot (\zeta_G(2) - 1)} + 30 \cdot q^{-\varepsilon}$, *where $d(r)$ depends only on r.*

(ii) *If r is bounded, then $\|P_{W_1} * P_{W_2} - U_G\|_1 \to 0$ as $|G| \to \infty$.*

Proof. Partition W_i into two subsets $W_{i,1}$ and $W_{i,2}$: $W_{i,1}$ will be the set of all regular semisimple elements in W_i, and $W_{i,2}$ will be the rest of the elements in W_i.

Then $W_{i,j}$ are normal subsets, and $W_i = W_{i,1} \cup W_{i,2}$, $W_{i,1} \cap W_{i,2} = \emptyset$.

Using inequality (1) in the proof of Theorem 3.3 for $k = 2$ we obtain:

$$\begin{aligned}\|P_{W_1} * P_{W_2} - U_G\|_1 \leq\ & \frac{|W_{1,1}|}{|W_1|}\frac{|W_{2,1}|}{|W_2|}\|P_{W_{1,1}} * P_{W_{2,1}} - U_G\|_1 \\ &+ \frac{|W_{1,1}|}{|W_1|}\frac{|W_{2,2}|}{|W_2|}\|P_{W_{1,1}} * P_{W_{2,2}} - U_G\|_1 \\ &+ \frac{|W_{1,2}|}{|W_1|}\frac{|W_{2,1}|}{|W_2|}\|P_{W_{1,2}} * P_{W_{2,1}} - U_G\|_1 \\ &+ \frac{|W_{1,2}|}{|W_1|}\frac{|W_{2,2}|}{|W_2|}\|P_{W_{1,2}} * P_{W_{2,2}} - U_G\|_1.\end{aligned}$$

We will handle the first summand differently from the other three summands.

The first summand:

$$\frac{|W_{1,1}|}{|W_1|}\frac{|W_{2,1}|}{|W_2|}\|P_{W_{1,1}} * P_{W_{2,1}} - U_G\|_1 \leq \|P_{W_{1,1}} * P_{W_{2,1}} - U_G\|_1.$$

$W_{1,1}$ and $W_{2,1}$ are normal subsets, and hence are unions of conjugacy classes. Denote these conjugacy classes of $W_{i,1}$ by $C_{i,1}, \ldots, C_{i,m_i}$. So $W_{i,1} = \bigcup_{j=1}^{m_i} C_{i,j}$.

Therefore, as in the proof of Theorem 3.3,

$$\|P_{W_{1,1}} * P_{W_{2,1}} - U_G\|_1 \leq \sum_{\substack{1 \leq j \leq m_1 \\ 1 \leq k \leq m_2}} \frac{|C_{1,j}||C_{2,k}|}{|W_{1,1}||W_{2,1}|}\|P_{C_{1,j}} * P_{C_{2,k}} - U_G\|_1.$$

By Lemma 2.12 there is a number $c(r)$, depending on r but not on q, such that $|\chi(x)| \leq c(r)$ for all $\chi \in \operatorname{Irr} G$ and all regular semisimple elements $x \in G$. Using Lemma 2.6 we obtain

$$\begin{aligned}\|P_{C_{1,j}} * P_{C_{2,k}} - U_G\|_1^2 &\leq \sum_{\substack{\chi \in \operatorname{Irr} G \\ \chi \neq 1}} \frac{|\chi(x_{1,j})|^2 |\chi(x_{2,k})|^2}{\chi(1)^2} \\ &\leq \sum_{\substack{\chi \in \operatorname{Irr} G \\ \chi \neq 1}} \frac{c(r)^4}{\chi(1)^2} = c(r)^4 \cdot (\zeta_G(2) - 1),\end{aligned}$$

where $C_{i,j} = x_{i,j}^G$ in the second expression.

Thus

$$\begin{aligned}\|P_{W_{1,1}} * P_{W_{2,1}} - U_G\|_1 &\leq \sum_{\substack{1 \leq j \leq m_1 \\ 1 \leq k \leq m_2}} \frac{|C_{1,j}||C_{2,k}|}{|W_{1,1}||W_{2,1}|} \|P_{C_{1,j}} * P_{C_{2,k}} - U_G\|_1 \\ &\leq \sqrt{c(r)^4 \cdot (\zeta_G(2) - 1)}.\end{aligned}$$

The other three summands:

According to Corollary 2.11, if we denote by $r(G)$ the proportion of regular semisimple elements in G, then $\frac{|W_{i,2}|}{|G|} \leq 1 - r(G) \leq \frac{5}{q}$.

We assume $\frac{|W_i|}{|G|} \geq q^{-(1-\varepsilon)}$.

Hence

$$\frac{|W_{i,2}|}{|W_i|} = \frac{\frac{|W_{i,2}|}{|G|}}{\frac{|W_i|}{|G|}} \leq 5 \cdot q^{-1+(1-\varepsilon)} = 5 \cdot q^{-\varepsilon}.$$

Since $\|P - Q\| \leq 2$ for distributions P and Q, we have

$$\begin{aligned}&\frac{|W_{1,1}|}{|W_1|}\frac{|W_{2,2}|}{|W_2|}\|P_{W_{1,1}} * P_{W_{2,2}} - U_G\|_1 + \frac{|W_{1,2}|}{|W_1|}\frac{|W_{2,1}|}{|W_2|}\|P_{W_{1,2}} * P_{W_{2,1}} - U_G\|_1 \\ &\quad + \frac{|W_{1,2}|}{|W_1|}\frac{|W_{2,2}|}{|W_2|}\|P_{W_{1,2}} * P_{W_{2,2}} - U_G\|_1 \leq 2\frac{|W_{2,2}|}{|W_2|} + 2\frac{|W_{1,2}|}{|W_1|} + 2\frac{|W_{1,2}|}{|W_1|} \\ &\quad \leq 6 \cdot 5 \cdot q^{-\varepsilon}.\end{aligned}$$

The sum:

$$\|P_{W_1} * P_{W_2} - U_G\|_1 \leq \sqrt{d(r) \cdot (\zeta_G(2) - 1)} + 30 \cdot q^{-\varepsilon},$$

proving (i).

In (ii) we assume that r is bounded, and so $d(r)$ is bounded. We also know from Theorem 2.9 that $\zeta_G(2) \to 1$ as $|G| \to \infty$. If r is bounded and $|G| \to \infty$ then $q \to \infty$, proving (ii). □

Notice that with these tools we cannot prove a better result for k normal subsets instead of 2.

For sets of the form $W = w(G)$ we now obtain:

Theorem 3.6. *Let $w \neq 1$ be a non-trivial group word. Let $G = G_r(q)$ be a finite simple group of Lie type of rank r over the field with q elements. Assume there exists $r_0(w)$, that may depend on w, such that $r \leq r_0(w)$. Then:*

(i) *There exist constants $N(w), d(w)$, depending only on w, such that if $|G| \geq N(w)$, then*

$$\|P_{w(G)} * P_{w(G)} - U_G\|_1 \leq \sqrt{d(w) \cdot (\zeta_G(2) - 1)} + 30 \cdot q^{-\frac{1}{2}}.$$

(ii) $\|P_{w(G)} * P_{w(G)} - U_G\|_1 \to 0$ *as* $|G| \to \infty$.

Proof. We are assuming that r is bounded by $r_0(w)$, so according to Theorem 2.1 there exists a constant $c(w) > 0$ that depends only on w such that $\frac{|w(G)|}{|G|} \geq c(w)$. Since we are assuming r is bounded, we have $q \to \infty$ as $|G| \to \infty$. So there exists $N(w)$ such that if $|G| \geq N(w)$ then $q^{-\frac{1}{2}} \leq c(w)$. So if $|G| \geq N(w)$ then $\frac{|w(G)|}{|G|} \geq c(w) \geq q^{-\frac{1}{2}}$.

We now apply Theorem 3.5 with $\varepsilon = 1/2$. Since $r \leq r_0(w)$ and $|G| \geq N(w)$, we have

$$\|P_{w(G)} * P_{w(G)} - U_G\|_1 \leq \sqrt{d(w) \cdot (\zeta_G(2) - 1)} + 30 \cdot q^{-\frac{1}{2}},$$

where $d(w)$ depends only on w, proving (i).

Part (ii) also follows since $\zeta_G(2) \to 1$ as $|G| \to \infty$, and since $q \to \infty$ as $|G| \to \infty$. □

Theorem 3.7. *Let $w \neq 1$ be a non-trivial group word and let G be a finite simple group. Then $\|P_{w(G)} * P_{w(G)} - U_G\|_1 \to 0$ as $|G| \to \infty$.*

Proof. According to 1.17 of [LaSh2], $\|P_{w(G)} * P_{w(G)} - U_G\|_1 \to 0$ as $|G| \to \infty$ if G is an alternating group.

For groups of Lie type use Theorems 3.4 and 3.6 to obtain the result.

Since $|G| \to \infty$ we can omit the sporadic groups.

According to the classification of finite simple groups this covers all of the finite simple group. □

Corollary 3.8. *Let k be a positive integer and let $w = x^k$. Let G be a finite simple group. Then $\|P_{w(G)} * P_{w(G)} - U_G\|_1 \to 0$ as $|G| \to \infty$.*

References

[Di1] P. Diaconis, *Group representations in probability and statistics*. IMS Lecture Notes—Monograph Ser. 11, Institute of Mathematical Statistics, Hayward, CA, 1988. Zbl 0695.60012 MR 0964069

[Di2] P. Diaconis, Random walks on groups: characters and geometry. In *Groups St Andrews 2001 in Oxford*, Vol. I, London Math. Soc. Lecture Note Ser. 304, Cambridge University Press, Cambridge 2003, 120–142. Zbl 1064.20071 MR 2051523

[DiS] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions. *Z. Wahrsch. verw. Gebiete* **57** (1981), 159–179. Zbl 0485.60006 MR 626813

[FuGu] J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. Preprint 2009. arXiv:0902.22381

[GaSh] S. Garion and A. Shalev, Commutator maps, measure preservation, and T-systems. *Trans. Amer. Math. Soc.* **361** (2009), 4631–4651. Zbl 1182.20015 MR 2506422

[Go] W. T. Gowers, Quasirandom groups. *Combin. Probab. Comput.* **17** (2008), 363–387. Zbl 1191.20016 MR 2410393

[GuLu] R. M. Guralnick and F. Lübeck, On p-singular elements in Chevalley groups in characteristic p. In *Groups and computation III*, Ohio State Univ. Math. Res. Inst. Publ. 8, de Gruyter, Berlin 2001, 169–182. Zbl 1001.20045 MR 1829478

[JaLi] G. James and M. Liebeck, *Representations and characters of groups*. Cambridge Math. Textbooks, Cambridge University Press, Cambridge 1993. Zbl 0792.20006 MR 1237401

[LanSe] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443. Zbl 0325.20008 MR 0360852

[La] M. Larsen, Word maps have large image. *Israel J. Math.* **139** (2004), 149–156. Zbl 1130.20310 MR 2041227

[LaSh1] M. Larsen and A. Shalev, Word maps and Waring type problems. *J. Amer. Math. Soc.* **22** (2009), 437–466. MR 2476780

[LaSh2] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications. *Invent. Math.* **174** (2008), 645–687. Zbl 1166.20009 MR 2453603

[LiSh1] M. W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications. *Ann. of Math.* (2) **154** (2001), 383–406. Zbl 1003.20014 MR 1865975

[LiSh2] M. W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties. *Invent. Math.* **159** (2005), 317–367. Zbl 1134.20059 MR 2116277

[LiSh3] M. W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type. *Proc. London Math. Soc.* (3) **90** (2005), 61–86. Zbl 1077.20020 MR 2107038

[Lul] N. Lulov, Random walks on symmetric groups generated by conjugacy classes. Ph.D. Thesis, Harvard University, Cambridge, MA, 1996.

[Lus] G. Lusztig, *Characters of reductive groups over a finite field*. Ann. of Math. Studies, Princeton University Press, Princeton 1984. Zbl 0556.20033 MR 0742472

[NiPy] N. Nikolov and L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem. *Europ. J. Math.*, to appear.

[Ser] J.-P. Serre, *Linear representations of finite groups*. Graduate Texts in Math. 42, Springer-Verlag, New York 1977. Zbl 0355.20006 MR 0450380

[Sh1] A. Shalev, Mixing and generation in simple groups. *J. Algebra* **319** (2008), 3075–3086. Zbl 1146.20057 MR 2397424

[Sh] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem. *Ann. of Math.* (2) **170** (2009), 1383–1416. Zbl 05710189 MR 2600876

Received April 30, 2009; revised August 25, 2009

G. Schul, A. Shalev, Institute of Mathematics, The Hebrew University, Jerusalem 91904, Israel

E-mail: gili.schul@mail.huji.ac.il; shalev@math.huji.ac.il